

McAfee Host Intrusion Prevention for Server

Präventiver Schutz für Ihre Server und Anwendungen

Hauptvorteile

Besserer Schutz

- Durchsetzung des breitesten Spektrums an IPS- und Zero-Day-Schutzmaßnahmen auf allen Servern und Ebenen: Netzwerk, Anwendung und Ausführung

Geringere Kosten

- Verringerung des Zeit- und Kostenaufwands mit einer leistungsstarken, zentralen Konsole für Ausbringung, Verwaltung, Reporting und Audits von Vorfällen, Richtlinien und Agenten
- Weniger häufige und dringliche Server-Patches

Einfachere Einhaltung

- Verwaltung der Einhaltung mit leicht verständlichen, umsetzbaren Ansichten, Workflows, Event-Monitoring und Reporting für prompte und gründliche Untersuchungen und Analysen

Die Herausforderung

Ihre Unternehmensserver beherbergen Ihre wertvollsten Datenbestände und halten Ihr Unternehmen am Leben. Für Sie als IT-Manager besteht eine der größten Herausforderungen darin, diese Server und Anwendungen vor bekannten und unbekanntem Angriffen zu schützen, die die Geschäftskontinuität bedrohen. Um dies zu erreichen, müssen Sie im gesamten Netzwerk aggressiv Sicherheitstechnologien implementieren.

Aber die Komplexität der Angriffe auf die Schwachstellen Ihrer Server und Anwendungen nimmt mit ebenso aggressiver Geschwindigkeit zu. In der ersten Hälfte des Monats Januar 2008 gab es mehr neue Bedrohungen als im gesamten Jahr 2007.¹ Und da mehr als 32 %² der Angriffe innerhalb von drei Tagen nach Entdeckung der betreffenden Schwachstelle erfolgen, sind besonders Unternehmen gefährdet. Denn durchschnittlich vergehen in Firmen 32 Tage bis zum Einspielen der Server-Patches.³ Es wird ein Schutz vor Zero-Day-Angriffen benötigt, um IT-Abteilungen die Sicherheit und Zeit zu verschaffen, Patches ordnungsgemäß zu priorisieren, zu planen, zu testen und bereitzustellen. Um dieses Spiel gewinnen zu können, ist die Einführung einer präventiven Sicherheitsstrategie vonnöten, die verhindert, dass es überhaupt zu Angriffen kommt. Mit einem präventiven Ansatz für den Schutz Ihrer Server und Anwendungen können Sie sicher sein, dass vertrauliche Daten geschützt sind und die Geschäftskontinuität erhalten bleibt.

McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention (Host IPS) überwacht und blockiert unerwünschte Aktivitäten und Bedrohungen. Die Server-Version von Host IPS hält die Server am Laufen und schützt Unternehmenswerte wie Anwendungen und Datenbanken. Host IPS schützt Server vor bekannten und Zero-Day-Bedrohungen durch die Kombination von signatur- und verhaltensorientiertem Intrusion Prevention-Schutz mit einer zustandsgesteuerten Desktop-Firewall und Anwendungskontrolle. McAfee Host IPS reduziert die Häufigkeit und Dringlichkeit von Patches, erhält die Geschäftstätigkeit und Mitarbeiterproduktivität, schützt die Vertraulichkeit von Daten und vereinfacht die Einhaltung von gesetzlichen Bestimmungen.

Verwaltbarkeit für Unternehmen

McAfee ePolicy Orchestrator® (ePO™) ist die branchenführende Plattform für die Verwaltung der Systemsicherheit, die Unternehmen einen koordinierten, präventiven Schutz vor Bedrohungen und Angriffen bietet. Mit ePO als Kern der McAfee-Lösungen für das Sicherheitsrisiko-Management (SRM) können Administratoren von einer zentralen, Web-basierten Konsole aus rund um die Uhr das Risiko unberechtigter, regelwidriger Systeme mindern, den Schutz aktuell halten, Sicherheitsrichtlinien einrichten und durchsetzen sowie den Schutzstatus überwachen. Implementieren Sie ePO und verwalten Sie Ihre gesamten neuen Sicherheitslösungen oder erweitern Sie Ihre Investitionen in unternehmensorientierte Lösungen für Sicherheitsmanagement und integrieren Sie Host IPS in Ihre bestehende ePO-Infrastruktur. Mit ePO lässt sich Host IPS leicht bereitstellen, konfigurieren und verwalten.

¹ McAfee Labs™

² McAfee Labs™

³ Forrester: The State of Server Operating System Security 2007 - Administrators Patch an Average of Eight Days Late (Der Sicherheitsstatus von Server-Betriebssystemen 2007 - Administratoren führen Patches durchschnittlich mit acht Tagen Verspätung durch), Juni 2007

Systemanforderungen

- Microsoft Windows (Englisch, Französisch, Deutsch, Spanisch, Japanisch, Koreanisch, traditionelles Chinesisch)
- Microsoft Windows 2000 Advanced Server ab Service Pack 3
- Microsoft Windows 2000 Datacenter Server ab Service Pack 3
- Microsoft Windows 2000 Professional ab Service Pack 3
- Microsoft Windows 2000 Server ab Service Pack 3
- Microsoft Windows Server 2003 Enterprise ab Service Pack 2, 32-Bit und 64-Bit
- Microsoft Windows Server 2003 R2 Enterprise, 32-Bit und 64-Bit
- Microsoft Windows Server 2003 Standard mit Service Pack 2, 32-Bit und 64-Bit
- Microsoft Windows Server 2003 R2 Standard, 32-Bit und 64-Bit
- Microsoft Windows Server 2003 Web ab Service Pack 1
- Microsoft Windows Server 2003 R2 Web
- Microsoft Windows Server 2008

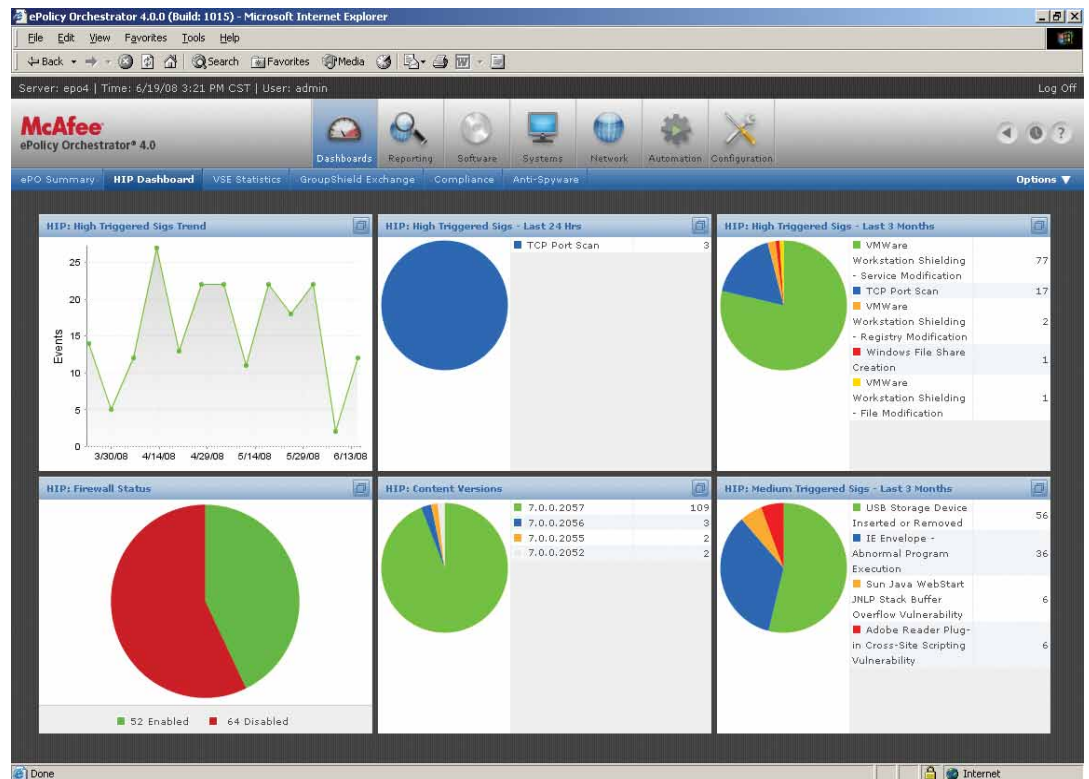
Funktionen und Vorteile

Mehrstufiger Schutz bietet eine breite, umfassende Abdeckung

Angesichts der schnellen Zunahme komplexer Bedrohungen und der profitorientierten Internet-kriminalität benötigen Unternehmen einen mehrstufigen Schutz, um ihre Endgeräte vor bekannten und Zero-Day-Bedrohungen zu schützen und den Verlust vertraulicher Daten zu verhindern.

- **Der signaturbasierte Schutz** identifiziert und blockiert bekannte Angriffe präzise
- **Der verhaltensbasierte Schutz** schützt Endgeräte vor neuen, Zero-Day-Bedrohungen wie z.B. Buffer Overflow-Angriffen
- **Die zustandsgesteuerte Firewall** blockiert unerwünschten eingehenden Datenverkehr, kontrolliert den ausgehenden Datenverkehr und wendet Richtlinien nach Datenverkehr, Ports, Anwendungen und Standorten an

- **Die Anwendungskontrolle** hilft Ihnen bei der Erstellung von Weiß- und Schwarzlisten, um festzulegen, welche Anwendungen ausgeführt werden dürfen und welche nicht
- **Der spezielle Server-Schutz** schützt wichtige Server mit kundenspezifischen Schutzmaßnahmen, um Systemverfügbarkeit und Produktivität aufrechtzuerhalten
 - Webserver
 - » Filterung von HTTP-Anfragen zur Verhinderung von Verzeichniswechsel-, Unicode- und Denial-of-Service-Angriffen
 - » Nutzung vordefinierter Schutzrichtlinien und -regeln zur Verhinderung von Angriffen und Datenverlust
 - Datenbankserver
 - » Untersuchung von Datenbank Anfragen zur Verhinderung von Angriffen wie SQL-Injektion
 - » Nutzung vordefinierter Schutzrichtlinien und -regeln zur Gewährleistung normalen Verhaltens und zur Verhinderung von Datenmanipulation



ePO-Dashboards erleichtern die Einsicht von Host IPS-Daten

Systemanforderungen (Forts.)

Red Hat Enterprise Linux 4.0 (nur 32-Bit)

Die folgenden Red Hat Enterprise Linux 4-Kernelmodule werden unterstützt:

- 2.6.9-22.EL
- 2.6.9-22.EL-smp
- 2.6.9-34.EL
- 2.6.9-34.EL-smp
- 2.6.9-42.EL
- 2.6.9-42.EL-smp

Sun Solaris

- SPARC Solaris 8 (32-Bit- oder 64-Bit-Kernel)
- SPARC Solaris 9 (32-Bit- oder 64-Bit-Kernel)
- SPARC Solaris 10

Unterstützte Web-Server-Plattformen

- IIS 4.0, 5.0 und 6.0 (Microsoft Windows)
- Apache 1.3.6 und späterer Webserver
- Apache 2.0.42 oder späterer Webserver
- Sun ONE Web Server 6.0
- Sun Java System Web Server 6.1

Unterstützte Datenbankserver-Plattformen

- Microsoft SQL Server 2000 (Windows) SP3a, SP4

Ihr IT-Team kann Patches seltener, weniger dringlich und nach eigenem Zeitplan durchführen

Ein großer Teil der Angriffe erfolgt innerhalb von drei Tagen nach Entdeckung einer Schwachstelle. Aber Unternehmen benötigen durchschnittlich 32 Tage, um Server-Patches zu implementieren. Host IPS schließt diese Sicherheitslücke und macht den Patch-Prozess einfacher und effizienter.

- **Der Schwachstellenschutz** aktualisiert Signaturen automatisch, um Endgeräte vor Angriffen auf Schwachstellen zu schützen
- **Der sofort aktive Schutz** kann eine überlegene Leistung aufweisen: Host IPS schützte 97 %⁴ aller im Jahr 2007 bekannt gewordenen Microsoft-Schwachstellen
- **Die Signatur-Updates** werden regelmäßig automatisch heruntergeladen, ähnlich wie .DAT-Datei-Updates, um den Schutz zu gewährleisten

ePO konsolidiert und zentralisiert die Verwaltung aller McAfee-Produkte

Unternehmen tun sich schwer mit den Kosten und dem Aufwand für die Verwaltung separater Sicherheitstechnologien auf ihren Endgeräten und in ihren Netzwerken. Durch die Verwendung einer einzigen, integrierten Sicherheitskonsole reduzieren Unternehmen die Anzahl der benötigten IT-Manager für die Verwaltung der Endgerätesicherheit um 44 %.⁵

- Zugriff auf zentrales Event-Monitoring, Berichte, Dashboards und Arbeitsabläufe mithilfe einer einzigen, Web-basierten Management-Konsole
- Bereitstellung, Verwaltung und Aktualisierung von Agenten und Richtlinien von einer Verwaltungsplattform aus

Geringerer Zeitaufwand für die Erfassung der Daten, die für Archivierung, Reporting und den Nachweis der Einhaltung benötigt werden

Die Einhaltung aufrechtzuerhalten und nachzuweisen kann eine Unmenge von IT-Ressourcen in Anspruch nehmen. Host IPS hilft Unternehmen dabei, mehr Transparenz und Kontrolle zu erhalten sowie die Einhaltung zu vereinfachen und den Aufwand für Reporting und Audits zu verringern.

- Erfassung von Angriffsdetails wie Art, Vektor, Quelle, Schwere, Zeitstempel usw., die in verständlicher Form dargestellt werden, für prompte Berichte, Audits, Untersuchungen und Gegenmaßnahmen
- Erstellung von Compliance-Berichten für Auditoren und andere Interessengruppen
- Anpassung von Dashboards für einen Compliance-Status in Echtzeit

⁴ McAfee Labs™

⁵ Insight Express, 2007

